Subject: [EXTERNAL] ATTORNEY GENERAL WILLIAM P. BARR DELIVERS KEYNOTE ADDRESS AT THE INTERNATIONAL CONFERENCE ON CYBER SECURITY

Date: Tuesday, July 23, 2019 at 9:36:36 AM Pacific Daylight Time

From: USDOJ-Office of Public Affairs

To: Farivar, Cyrus (NBCUniversal)

seal - centered header for gov delivery

The United States Department of Justice

FOR IMMEDIATE RELEASE TUESDAY, JULY 23, 2019

ATTORNEY GENERAL WILLIAM P. BARR DELIVERS KEYNOTE ADDRESS AT THE INTERNATIONAL CONFERENCE ON CYBER SECURITY

New York, NY

Remarks as prepared for delivery

Good Morning.

Thank you all for being here this morning. I would like to offer particular thanks to Fordham University for hosting this Conference and this morning's opening ceremony. As a native New Yorker, it is always nice to have a good excuse to be in the City.

I would also like to thank the New York Division of the FBI for their work in putting on this Conference.

Of all that has changed over the last 30 years, cyber-related issues and cybersecurity may well be the most significant difference between my first tenure as Attorney General and this one. Since taking office in February, I have spent a significant amount of time getting up to speed on the developments in this important area. And I have been both impressed and reassured as I have learned about all of the investment and effort that makes the FBI a leader in this area.

As individuals and as a nation we have become dependent on a vast and expanding digital infrastructure. That, in turn, has made us vulnerable to cybercriminals and foreign adversaries that target that infrastructure. The danger cannot be overstated, and enhancing cybersecurity is a national imperative — one shared by the private sector whose networks, data systems and products are at risk, as well as the government agencies charged with securing our critical national infrastructure and guarding our citizens against criminal activity. Among the most critical advances in cybersecurity has been the development of advanced encryption techniques and their deployment in a range of important applications. Encryption provides enormous benefits to society by enabling secure communications, data storage and on-line transactions. Because of advances in encryption, we can now better protect our personal information; more securely engage in e-commerce and internet

communications; obtain secure software updates; and limit access to sensitive computers, devices, and networks.

As the Federal Government, we welcome these improvements to privacy and security, and will work to preserve and strengthen them. But at the same time, we must recognize that our citizens face an array of threats to their safety far broader than just cyber threats. Hackers are a danger, but so are violent criminals, terrorists, drug traffickers, human traffickers, fraudsters, and sexual predators. While we should not hesitate to deploy encryption to protect ourselves from cybercriminals, this should not be done in a way that eviscerates society's ability to defend itself against other types of criminal threats. In other words, making our virtual world more secure should not come at the expense of making us more vulnerable in the real world. But, unfortunately, this is what we are seeing today.

Service providers, device manufacturers and application developers are developing and deploying encryption that can only be decrypted by the end user or customer, and they are refusing to provide technology that allows for lawful access by law enforcement agencies in appropriate circumstances. As a result, law enforcement agencies are increasingly prevented from accessing communications in transit or data stored on cell phones or computers, even with a warrant based on probable cause to believe that criminal activity is underway. Because, in the digital age, the bulk of evidence is becoming digital, this form of "warrant proof" encryption poses a grave threat to public safety by extinguishing the ability of law enforcement to obtain evidence essential to detecting and investigating crimes. It allows criminals to operate with impunity, hiding their activities under an impenetrable cloak of secrecy. As you know, some refer to this eclipsing of the Government's investigative capabilities as "going dark." While encryption protects against cyberattacks, deploying it in warrant-proof form jeopardizes public safety more generally. The net effect is to reduce the overall security of society. I am here today to tell you that, as we use encryption to improve cybersecurity, we must ensure that we retain society's ability to gain lawful access to data and communications when needed to respond to criminal activity.

This proposition should not be controversial. It simply reflects the balance struck in the Constitution itself and maintained since the Founding era. The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment strikes a balance between the individual citizen's interest in conducting certain affairs in private and the general public's interest in subjecting possible criminal activity to investigation. It does so, on the one hand, by securing for each individual a private enclave around his "person, house, papers, and effects" — a "zone" bounded by the individual's own reasonable expectations of privacy. So long as the individual acts within this "zone of privacy," his activities are shielded from unreasonable Government investigation. On the other hand, the Fourth Amendment establishes that, under certain circumstances, the public has a legitimate need to gain access to an individual's zone of privacy in pursuit of public safety, and it defines the terms under which the Government may obtain that access. When the Government has probable cause to believe that evidence of a crime is within an individual's zone of privacy, the Government is entitled to search for or seize the evidence, and the search usually must be preceded by a judicial determination that "probable cause" exists and be authorized by a warrant.

The key point is that the individual's right to privacy and the public's right of access are two sides of the same coin. The reason we are able, as part of our basic social compact, to guarantee individuals a certain zone of privacy is precisely because the public has reserved the right to access that zone when public safety requires. If the public's right of access is blocked, then these zones of personal privacy are converted into "law-free zones" insulated from legitimate scrutiny.

Since the Founding, advances in technology have disrupted this balance in different ways. Sometimes, technology creates new spheres of privacy that the drafters of the Fourth Amendment could not have thought to enumerate, such as with the advent of the telephone. Sometimes, technology gives law enforcement new means to invade privacy that were previously unimaginable, such as thermal imaging devices. And sometimes, technology makes it easier for suspects to evade law enforcement even when there is a lawful basis to investigate, such as automobiles — or to bring us back today's topic, data encryption.

With each of these earlier examples, our society has ensured that the traditional balance between individual privacy and public safety was maintained, as reflected in rulings from the Supreme Court. In *Katz v. United States* (1967), the Court held that the Fourth Amendment applied to government bugging of a phone booth — even though this technique did not strictly involve a search of the suspect's person, house, papers, or effects. Decades later in *Kyllo v. United States* (2001), the Court held that the Fourth Amendment applied to the use of a thermal imaging device to look inside a home — even though prior doctrine strongly suggested that government exploitation of light waves emitted from the property was outside the scope of Fourth Amendment protection. The Supreme Court's application of Fourth Amendment protection to the attachment of a GPS tracking device to a car in *United States v. Jones* (2012) had a similar effect. In each of these cases, the Court protected privacy against advances in technology. But of course, law enforcement retained the ability to bug a phone booth, to use thermal imaging on a house, or to attach a GPS device to a car if a warrant issued first.

The same script has played out in reverse, with the Supreme Court taking steps to ensure that advances in technology do not unduly tip the scales against public safety by preventing effective law enforcement. A notable example concerns automobiles. If the zone of privacy was extended to automobiles — as a type of personal "effect" or mobile "house" — then it would be difficult, if not impossible, for law enforcement to work within the traditional requirement that police obtain a warrant from a neutral magistrate before conducting a search or seizure. Even when an officer had probable cause to seize a car and search its contents, the driver could get away long before the officer could complete the process to obtain a warrant. This development threatened again to disrupt the traditional balance between individual privacy and public safety.

So what did we do? In a series of decisions that started with *Carroll v. United States* (1925), the Supreme Court articulated an exception to the traditional warrant requirement which allows police to seize and search a car without a warrant so long as it can later be shown that they had probable cause to support the investigation. In other words, we did not make automobiles law-free zones. We preserved the constitutional balance by ensuring that law enforcement retained the practical capability to conduct a search when lawfully predicated.

The point I hope you take away today is that our societal response to advances in technology that affect the balance between individual privacy and public safety always has been — and

always should be — a two-way street. When these advances tip the scales too far in favor of the Government, the response is to expand privacy protections. And when these advances threaten public safety by thwarting effective law enforcement, the response should be to preserve lawful access.

By enabling dangerous criminals to cloak their communications and activities behind an essentially impenetrable digital shield, the deployment of warrant-proof encryption is already imposing huge costs on society. It seriously degrades the ability of law enforcement to detect and prevent crime before it occurs. And, after crimes are committed, it thwarts law enforcement's ability to identify those responsible or to successfully prosecute the guilty parties. These costs will grow exponentially as deployment of warrant-proof encryption accelerates and criminals are emboldened by their ability to evade detection.

At conferences like this, we talk about those costs in abstract terms. They are not abstract; they are real. The costs of irresponsible encryption that blocks legitimate law enforcement access is ultimately measured in a mounting number of victims — men, women, and children who are the victims of crimes — crimes that could have been prevented if law enforcement had been given lawful access to encrypted evidence. Law enforcement has generally not wanted to get too specific about these cases because details can help sophisticated criminals and terrorists evade detection. But, given the frequency with which these situations are now arising, it is only a matter of time before a sensational case crystalizes the issue for the public. FBI Director Wray will be speaking later in the week at this Conference and will address some of the damage being inflicted on law enforcement by encryption that blocks lawful access. But, for now, I want to make a couple of points about the extent of the harm.

Like everybody else, criminals of all stripes increasingly rely on wireless communications, hand-held devices, and the internet. This is especially true of larger-scale criminal organizations that need to coordinate many conspirators over a wide geographical area. Thus, we have seen transnational drug cartels increasingly move their communications onto commercially available encrypted platforms designed to block lawful access. One of many examples is a Mexican cartel that recently started trafficking large quantities of finished fentanyl from Asia to Mexico and then to the United States. The cartel started using WhatsApp as their primary communication method, preventing U.S. law enforcement from conducting wiretaps that would enable us to locate fentanyl shipments and seize them at the border. We also found that the cartel had used WhatsApp for the specific purpose of coordinating the murders of Mexico-based police officials. The cartel ended up murdering hundreds of these police officers. Had we been able to gain lawful access to the chat on a timely basis, we could have saved these lives. So the costs of not being able to gain lawful access in this case were the lives of the assassinated officers, as well as the many lives impacted here by unimpeded entry into the United States of huge amounts of deadly fentanyl.

This is just one of countless examples involving the drug war. Indeed, just the damage done by warrant-proof encryption to our ability to combat drug trafficking is a cost too high to pay. The tsunami of opioids, cocaine, and methamphetamine that started surging into the United States from Mexico in the latter years of the Obama Administration is one of the greatest dangers to the wellbeing of our Nation that we face today. In a single year, more Americans die from drug overdoses than we lost in the entire Vietnam War. In addition to this death toll, hundreds of thousands of lives are destroyed. The vast majority of the drugs are trafficked into the United States by large, transnational criminal organizations. In times past, when we had considerable success in combating similar cartels, the indispensable tool was

communications intelligence. It remains the indispensable tool today. If our law enforcement agencies do not recover the ability to gain lawful access to encrypted communications and platforms, the prospects of successfully prosecuting the drug war by traditional law enforcement means are dim.

Warrant-proof encryption is also seriously impairing our ability to monitor and combat domestic and foreign terrorists. As with drug cartels, we are seeing terrorist organizations moving their communications to encrypted platforms designed to block lawful access. Even smaller terrorist groups and "lone wolf" actors have turned increasingly to encryption. The 2015 terrorist attack in Garland, Texas still rankles. There, two Islamist extremists carried out an attack for which ISIS claimed responsibility. On the morning of the attack, one of the terrorists exchanged approximately 100 instant messages with an overseas terrorist using an end-to-end encrypted app. To this date, the FBI has still not been able to determine the content of these messages. The deployment of warrant-proof encryption is diminishing the communications intelligence we are able to collect on terrorist threats. Due to the very nature of terrorism – where each actor seeks to inflict high casualties – encryption that allows terrorists to operate beyond the reach of lawful surveillance poses an unacceptable risk to the country.

One further point about the costs imposed on society by warrant-proof encryption: it is not only about the crimes that could have been avoided, or the criminals that escape punishment. Converting the internet and communication platforms into "law free" zones, and thus giving criminals the means to operate free of lawful scrutiny, will inevitably propel an expansion of criminal activity. If you remove any possibility that the cops are going to be watching a neighborhood, the criminals already in the neighborhood will commit a lot more crimes.

The "going dark" problem is not limited to terrorism or drug cartel cases. While those cases are vitally important, it is also important that law enforcement at the federal, state, and local level retain the ability to investigate and prosecute the full spectrum of crimes that plague society. We are aware, for example, that a large violent gang is using encrypted apps to "green light" assassinations, and yet, because we cannot access the messages, we cannot prevent the murders. We also know that human traffickers and pedophiles use the internet to facilitate their crimes, and yet encryption is impairing our visibility into some of these activities. With the growing availability of commoditized encryption, it is becoming easier for common criminals to communicate beyond the reach of traditional surveillance. This problem is becoming especially acute for our State and local partners, who lack the resources of the federal government, and whose ability to investigate and prosecute crime is being seriously impaired by warrant-proof encryption.

The Department has made clear what we are seeking. We believe that when technology providers deploy encryption in their products, services, and platforms they need to maintain an appropriate mechanism for lawful access. This means a way for government entities, when they have appropriate legal authority, to access data securely, promptly, and in an intelligible format, whether it is stored on a device or in transmission. We do not seek to prescribe any particular solution. Our private-sector technology providers have immensely talented engineers who have built the very products and services that we are talking about. They are in the best position to determine what methods of lawful access work best for their technology. But there have been enough dogmatic pronouncements that lawful access simply cannot be done. It can be, and it must be.

We are confident that there are technical solutions that will allow lawful access to encrypted

data and communications by law enforcement without materially weakening the security provided by encryption. Such encryption regimes already exist. For example, providers design their products to allow access for software updates using centrally managed security keys. We know of no instance where encryption has been defeated by compromise of those provider-maintained keys. Providers have been able to protect them.

We think our tech sector has the ingenuity to develop effective ways to provide secure encryption while also providing secure legal access. Some good minds have already started to focus on this, and some promising ideas are emerging. Our colleagues from GCHQ have proposed "Virtual Alligator Clips" which allow a provider to respond to a warrant by adding a silent law enforcement recipient to an otherwise secure chat. Ray Ozzie has tabled a proposal for "Exceptional Access Keys" for locked, encrypted phones so they can be unlocked pursuant to a warrant. Matt Tait has proposed Layered Cryptographic Envelopes to allow lawful access to encrypted data-at-rest on disks or other storage devices. I am sure that the putative shortcomings of these ideas have been identified, which hopefully will spur further refinements and alternative proposals. Through this dialectic we can identify workable solutions. I am not endorsing any particular solution. And we will likely need different kinds of solutions for communications and data in transit, as opposed to data at rest. But I am suggesting that it is well past time for some in the tech community to abandon the indefensible posture that a technical solution is not worth exploring and instead turn their considerable talent and ingenuity to developing products that will reconcile good cybersecurity to the imperative of public safety and national security. As Microsoft's Bill Gates has observed, "[t]here's no question of ability; it's the question of willingness."

Some object that requiring providers to design their products to allow for lawful access is incompatible with some companies' "business models." But what is the business objective of the company? Is it "A" — to sell encryption that provides the best protection against unauthorized intrusion by bad actors? Or is it "B" — to sell encryption that assures that law enforcement will not be able to gain lawful access? I hope we can all agree that if the aim is explicitly "B" — that is, if the purpose is to block lawful access by law enforcement, whether or not this is necessary to achieve the best protection against bad actors — then such a business model, from society's standpoint, is illegitimate, and so is any demand for that product. The product jeopardizes the public's safety, with no countervailing utility. Few companies would say this is their goal.

On the other hand, it is contended that achieving "B" (the blocking of lawful access) is essential to achieving "A" (giving the best protection against bad actors). Thus, the argument is that a business is thwarted in its purpose of offering the best protection against bad actors unless it can also override society's interest in retaining lawful access. Some hold this view dogmatically, claiming that it is technologically impossible to provide lawful access without weakening security against unlawful access. But, in the world of cybersecurity, we do not deal in absolute guarantees but in relative risks. All systems fall short of optimality and have some residual risk of vulnerability — a point which the tech community acknowledges when they propose that law enforcement can satisfy its requirements by exploiting vulnerabilities in their products. The real question is whether the residual risk of vulnerability resulting from incorporating a lawful access mechanism is materially greater than those already in the unmodified product. The Department does not believe this can be demonstrated.

Moreover, even if there was, in theory, a slight risk differential, its significance should not be judged solely by the fact it falls short of theoretical optimality. Particularly with respect to

encryption marketed to consumers, the significance of the risk should be assessed based on its practical effect on consumer cybersecurity, as well as its relation to the net risks that offering the product poses for society. After all, we are not talking about protecting the Nation's nuclear launch codes. Nor are we necessarily talking about the customized encryption used by large business enterprises to protect their operations. We are talking about consumer products and services such as messaging, smart phones, e-mail, and voice and data applications. If one already has an effective level of security — say, by way of illustration, one that protects against 99 percent of foreseeable threats — is it reasonable to incur massive further costs to move slightly closer to optimality and attain a 99.5 percent level of protection even where the risk addressed is extremely remote? A company would not make that expenditure; nor should society. Here, some argue that, to achieve at best a slight incremental improvement in security, it is worth imposing a massive cost on society in the form of degraded public safety. This is untenable, again using a crude illustration, if the choice is between a world where we can achieve a 99 percent assurance against cyber threats to consumers, while still providing law enforcement 80 percent of the access it might seek; or a world, where we have boosted our cybersecurity to 99.5 percent but at a cost reducing law enforcements access to zero percent — the choice for society is clear.

Some who resist lawful access complain it places an unreasonable burden on companies, who must spend time and resources on developing and implementing a compliance mechanism. To that, I first say, "Welcome to civil society." We regularly expect — and often mandate if necessary — that our companies take steps to ensure that their products and services do not impose negative externalities on the public interest. Sometimes this requires prohibiting certain products all together; other times it requires modification of products so they are compatible with the public interest.

Further, the burden is not as onerous as some make it out to be. I served for many years as the general counsel of a large telecommunications concern. During my tenure, we dealt with these issues and lived through the passage and implementation of CALEA — the Communications Assistance for Law Enforcement Act. CALEA imposes a statutory duty on telecommunications carriers to maintain the capability to provide lawful access to communications over their facilities. Companies bear the cost of compliance but have some flexibility in how they achieve it, and the system has by and large worked. It is absurd to think that we would preserve lawful access by mandating that physical telecommunications facilities be accessible to law enforcement for the purpose of obtaining content, while allowing tech providers to block law enforcement from obtaining that very content.

The United States is not alone in addressing this issue. In fact, many of our international partners such as the UK and Australia are already moving on statutory frameworks to address it. China and Russia have their predictable approach, American companies have an opportunity to advance their interests by setting industry standards now that can influence the conversation here and worldwide in the years to come.

Obviously, the Department would like to engage with the private sector in exploring solutions that will provide lawful access. While we remain open to a cooperative approach, the time to achieve that may be limited. Key countries, including important allies, have been moving toward legislative and regulatory solutions. I think it is prudent to anticipate that a major incident may well occur at any time that will galvanize public opinion on these issues. Whether we end up with legislation or not, the best course for everyone involved is to work soberly and in good faith together to craft appropriate solutions, rather than have outcomes

dictated during a crisis. As this debate has dragged on, and deployment of warrant-proof encryption has accelerated, our ability to protect the public from criminal threats is rapidly deteriorating. The status quo is exceptionally dangerous, unacceptable, and only getting worse. The rest of the world has woken up to this threat. It is time for the United States to stop debating *whether* to address it, and start talking about *how* to address it.

# # #

AG

19-796

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.